REMARKS

35 USC §112 Claim Rejections.

3. The Office Action states that "Claims 30-38 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP §2172.01. The omitted steps are: purchasing the asset and tracking and storing a client usage of content. Claims 31-38 are also rejected as each depends from claim 30."

Applicant has amended Claim 30, to claim a process, comprising the steps of:

purchasing usage rights for an encrypted asset by sending purchase information from a client machine to a store server;

sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the encrypted asset;

sending an asset request for the encrypted asset using the asset ID from the client machine to a fulfillment server;

sending the encrypted asset from the fulfillment server to the client machine in response to the received asset ID;

sending a license request from the client machine to the fulfillment server;

sending a license from the fulfillment server to the client machine, the license comprising an asset key and the usage rights associated with the encrypted asset;

encrypting the asset key and the usage rights at the client machine;

binding the encrypted asset key to the client machine;

combining the machine-bound encrypted asset key and encrypted user rights into machine-bound asset rights;

storing the machine-bound asset rights within a secure key locker within the client machine;

sending an acknowledgement of the receipt of the encrypted asset and the license from the client machine to the fulfillment server;

receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use.

Support is seen in the Application as filed, at least on [0021], [0038]-[0040], [0042]-[0043], [0052], [0054], [0059], [0060]-[0062], [0064]-[0065], [0067], [0071]-0072], [0074], [0076]; and in Figures 1, 3-5, and 9.

Applicant notes that Claim 30, as amended, comprises the step of, *inter alia*:

"purchasing usage rights for an encrypted asset by sending purchase information from a client machine to a store server".

Specific support is seen in the Application as filed, at least in [0054]; in Figure 1 (*e.g.* element 3, and purchase transaction 34); and in Figure 3 (*e.g.* element 166: member purchases song from the Digital Store).

Applicant also notes that Claim 30, as amended, comprises the steps of, *inter alia*:

"receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights"; and

"conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights".

Specific support is seen in the Application as filed, at least in [0062], [0064]-[0065], [0067], [0072], [0074]-[0076].

Applicant submits that Claim 30, as amended, overcomes the rejections under 35 U.S.C. 112, second paragraph.

4. The Office Action also states that "Claims 30-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Office Action states that "Claim 30 recites "*controlling usage* of the purchase asset..." and "updating the usage rights... in accordance to the *controlled usage*" (emphasis added). The term "controlling usage", however, is not necessarily an action, a step or a positive recitation. For example, while a door "controls" who can enter a room, it does not actively [perform] a step of "controlling" (i.e. hanging is not controlling). Therefore, absent a step of tracking how usage of the asset is controlled (e.g. computer prevented a user's attempt to send the asset to another) or at least how the asset is used (e.g. played four times) Applicant's "updating" step is unclear to one of ordinary skill (In re Zletz, 13 USPQ2d 1320 (Fed. Cir. 1989))."

The Office Action also states that "Claim 30 recites the limitations "the purchased asset" and "the controlled usage" in lines 4 and 16-17, respectively. There is insufficient basis for these limitations in the claim. Claims 31-38 are also rejected as each depends from claim 30."

Applicant has amended Claim 30, to particularly point out and distinctly claim a process, comprising the steps of:

purchasing usage rights for an encrypted asset by sending purchase information from a client machine to a store server;

sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the encrypted asset;

sending an asset request for the encrypted asset using the asset ID from the client machine to a fulfillment server;

sending the encrypted asset from the fulfillment server to the client machine in response to the received asset ID;

sending a license request from the client machine to the fulfillment server;

sending a license from the fulfillment server to the client machine, the license comprising an asset key and the usage rights associated with the encrypted asset;

encrypting the asset key and the usage rights at the client machine;

binding the encrypted asset key to the client machine;

combining the machine-bound encrypted asset key and encrypted user rights into machine-bound asset rights;

storing the machine-bound asset rights within a secure key locker within the client machine;

sending an acknowledgement of the receipt of the encrypted asset and the license from the client machine to the fulfillment server;

receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use.

Support is seen in the Application as filed, at least in [0021], [0038]-[0040], [0042]-[0043], [0052], [0054], [0059], [0060]-[0062], [0064]-[0065], [0067], [0071]-0072], [0074], [0076]; and in Figures 1, 3-5, and 9.

Applicant submits that Claim 30, as amended, does not use the terminology "controlled usage", and that the claim positively cites the steps of, *inter alia*:

"conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use".

Applicant submits that Claim 30, as amended, particularly points out and distinctly claims the subject matter of one the preferred embodiments, and is clear to one of ordinary skill in the art. Therefore, Applicant submits that Claim 30, as amended, overcomes the rejection under 35 U.S.C. 112, second paragraph. As Claims 31-38 depend to Claim 30, as amended, they are seen to overcome the rejections as well.

35 USC §103 Claim Rejections.

6. The Office Action states that "Claims 30-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al. (U.S. Patent No. 6,772,340) in view of Milsted at al. (U.S. Patent No. 6,263,313)."

The Office Action concedes that "Peinado et al. do not specifically recite a ticket comprising an asset ID that corresponds to the purchased asset".

However, the Office Action also states that "Milsted et al. [teaches] sending a ticket (comprising an asset ID of a purchased asset) from a server (figures 1A-D; column 14, lines 10-15) to a client machine, sending a request for the purchased asset using the asset ID from the client machine to the server, and in response, the server sending the asset to the client machine (column 20, lines 61-67; column 21, lines 15-30; column 39, lines 6-50; column 70, lines 40-65; column 83, lines 35-45)."

The Office Action also states "Milsted et al. also teach sending a license request to the server (column 21, lines 22-48) and sending an acknowledgement of the receipt of the license and the asset (column 79, lines 5-23)."

Hilton Davis / Festo Statement

Applicant has amended Claim 30, for convenience in prosecution, and reserves the right to present the same or similar claims in a related Application. The amendments herein were not made for any reason related to patentability.

Applicant has amended Claim 30, to particularly point out and distinctly claim a process, comprising the steps of:

purchasing usage rights for an encrypted asset by sending purchase information from a client machine to a store server;

sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the encrypted asset;

sending an asset request for the encrypted asset using the asset ID from the client machine to a fulfillment server;

sending the encrypted asset from the fulfillment server to the client machine in response to the received asset ID;

sending a license request from the client machine to the fulfillment server;

sending a license from the fulfillment server to the client machine, the license comprising an asset key and the usage rights associated with the encrypted asset;

encrypting the asset key and the usage rights at the client machine;

binding the encrypted asset key to the client machine;

combining the machine-bound encrypted asset key and encrypted user rights into machine-bound asset rights;

storing the machine-bound asset rights within a secure key locker within the client machine;

sending an acknowledgement of the receipt of the encrypted asset and the license from the client machine to the fulfillment server;

receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use.

Support is seen in the Application as filed, at least in [0021], [0038]-[0040], [0042]-[0043], [0052], [0054], [0059], [0060]-[0062], [0064]-[0065], [0067], [0071]-0072], [0074], [0076]; and in Figures 1, 3-5, and 9.

Peinado at al. describe a digital rights management system operating on computing device and having black box tied to computing device, as seen at least in the Abstract, wherein:

> "A digital rights management (DRM) system operates on a computing device when a user requests that an encrypted piece of digital content be rendered by the computer device. The computing device has an identifier. A black box performs decryption and encryption functions in the DRM system. The black box includes a key file and an executable. The key file includes at least one black box public key and is expected to include the identifier of the computing device, the black box thus being tied to the computing device by inclusion of such first identifier. A digital license corresponding to the digital content is resident in the DRM system and includes a decryption key for decrypting the encrypted digital content. The decryption key is expected to be encrypted according to a black box public key of the key file of the black box, the license thus being tied to the black box and by extension the computing device. If the identifier of the computing device is in fact different than the identifier in the key file of the black box, a different key file is produced based on the black box public key(s) of the key file and the different identifier of the computing device."

Peinado describe basic distribution of encrypted content, and also describe that a decrypting key may be included with a license (16), as seen at least in column 5, lines 25-30:

> "The digital content 12 is distributed in an encrypted form, and may be distributed freely and widely. Preferably, the decrypting key (KD) for decrypting the digital content 12 is included with the license 16."

Peinado also describe a trusted component or mechanism (32) that is provided by the user's computing device (14), such that the computing device (14) will not render the digital content (12) except according to the license rules embodied in the license (16), as seen at least in column 13, lines 9-19, wherein:

> "The content owner for a piece of digital content 12 must trust that the user's computing device 14 will abide by the rules specified by such content owner, i.e. that the digital content 12 will not be rendered unless the user obtains a license 16 that permits the rendering in the manner sought. Preferably, then, the user's computing device 14 must provide a trusted component or mechanism 32 that can satisfy to the content owner that such computing device 14 will not render the digital content 12 except according to the license rules embodied in the license 16 associated with the digital content 12 and obtained by the user."

As well, Peinado generally describe a "rights description in each license", as seen at least in column 17, line 60 to column 18, line 8:

> "As should be understood, the rights description in each license 16 specifies whether the user has rights to play the digital content 12 based on any of several factors, including who the user is, where the user is located, what type of computing device 14 the user is using, what rendering application 34 is calling the DRM system 32, the date, the time, etc. In addition, the rights description may limit the license 16 to a pre-determined number of plays, or pre-determined play time, for example. In such case, the DRM system 32 must refer to any state information with regard to the license 16, (i.e., how many times the digital content 12 has

been rendered, the total amount of time the digital content 12 has been rendered, etc.), where such state information is stored in the state store 40 of the DRM system 32 on the user's computing device 14."

In regard to Claim 30, as amended, Applicant submits that, while Peinado generally describe a "rights description in each license", and that a trusted component or mechanism (32) is provided by the user's computing device (14), there is no disclosure in Peinado, or suggestion, express or implied, of a process that comprises the steps of, *inter alia*:

"receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use."

Applicant also submits that, while Peinado generally describe distribution of content packages, as seen at least in column 10, lines 3-18; in column 14, lines 44-57; and in column 17, lines 5-12, Peinado fails to teach or suggest a need for any of "sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the encrypted asset"; or "sending an asset request for the encrypted asset using the asset ID from the client machine to a fulfillment server".

As well, even though Milsted generally describe secure containers (SC) for some transactions, as seen at least in column 21, lines 15-30 and on Col. 39, lines 6-50, there is an absence of motivation to modify Peinado to include secure containers (SC) for such transactions, such as to build an "order SC that contains among other things the Encrypted Symmetric Key for the Content 113, the Transaction ID, and End-User(s) information".

Furthermore, Applicant submits that Milsted does not remedy the shortcomings of Peinado, such that, even in combination, Claim 30, as amended, is patentable over Peinado in view of Milsted.

Milsted describe a method and apparatus to create encoded digital content, as seen at least in the Abstract, wherein:

> "A method of automatically selecting processing parameters for encoding digital content. Metadata containing the genre of the digital content, receiving the compression level selected for encoding the digital content is received. An algorithm selected for encoding the digital content is received. And a previously defined table to select the processing parameters for encoding the digital content based on the genre of the

content, the compression level selected and the algorithm selected is indexed and the processing parameters are retrieved. In accordance with another aspect of the invention, an apparatus is described to carry out the above method"

In regard to Claim 30, as amended, Applicant submits that, while Milsted describes secure containers (SC) for distribution of encrypted content and information among the system components, as seen at least in column 9, line 66 to col. 10, line 7, there is no disclosure in Milsted, or suggestion, express or implied, of "a process, comprising the steps of:

purchasing usage rights for an encrypted asset by sending purchase information from a client machine to a store server;

sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the encrypted asset;

sending an asset request for the encrypted asset using the asset ID from the client machine to a fulfillment server;

sending the encrypted asset from the fulfillment server to the client machine in response to the received asset ID;

sending a license request from the client machine to the fulfillment server;

sending a license from the fulfillment server to the client machine, the license comprising an asset key and the usage rights associated with the encrypted asset;

encrypting the asset key and the usage rights at the client machine;

binding the encrypted asset key to the client machine;

combining the machine-bound encrypted asset key and encrypted user rights into machine-bound asset rights;

storing the machine-bound asset rights within a secure key locker within the client machine;

sending an acknowledgement of the receipt of the encrypted asset and the license from the client machine to the fulfillment server;

receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use."

For example, Applicant submits that, while Milsted describes secure containers (SC) for distribution of encrypted content and information among system components, there is no disclosure in Milsted, or suggestion, express or implied, of a process, comprising the steps of, *inter alia*:

"receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use."

Applicant therefore respectfully submits that, even in combination, Peinado and Milsted fail to meet Claim 30, as amended. As well, it would take significant modification and undue experimentation to meet Claim 30, as amended, based on any of Peinado and/or Milsted.

Therefore, the *prima facie* obviousness case is incomplete because Peinado and Milsted fail to teach or suggest all the claim limitations (MPEP 2142, 2143.03). To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references (Ex Parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985), MPEP 706.02(j)). As well, the Examiner should "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this

analysis should be made explicit (*KSR Int'l Co., v. Teleflex, Inc.*, No 04-1350 (U.S. Apr. 30, 2007)).

Applicant therefore submits that independent Claim 30, as amended, overcomes the rejection under 35 U.S.C. §103(a) as being unpatentable over Peinado in view of Milsted.

As Claims 31-38 depend from amended independent Claim 30, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

Other Amendments.

Applicant has amended the Specification and Claim 37, to correct grammatical errors. Applicant has also amended Claims 31 and 34-38, to provide proper antecedent terminology.

Furthermore, Applicant has entered new dependent Claims 59-61, to further point out and distinctly claim preferred embodiments. Support is seen in the Application as filed, at least in Figure 13 and in [0053], [0075], [0080], and [0099].

Applicant has also entered new dependent Claims 62-64, to further point out and distinctly claim preferred embodiments. Support is seen in the Application as filed, at least in Figures 1, 3, 4, and 16; in [0021], [0043]-[0044], [0052]-[0053], [0072]-[0081], [0090]-[0096], [0109], and [0019]-[0020]; and in dependent Claims 11, 13, and 15.

Applicant has also entered new dependent Claim 65, to further point out and distinctly claim "the process of Claim 30, further comprising the step of:

launching a download manager at the client machine with the received ticket;

wherein the asset request is sent from the launched download manager at the client machine to the fulfillment server."

Support is seen in the Application as filed, at least in Figures 3-5; and in [0055] and [0057]-[0058].

As Claims 59-65 depend from amended independent Claim 30, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

CONCLUSION

Applicant submits that the claims in the present application are directed to statutory subject matter. Applicant submits that this amendment does not introduce new matter into the Application. Based on the foregoing, Applicant considers the invention to be in condition for allowance. Applicant earnestly solicits the Examiner's withdrawal of the rejection set forth in the prior Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States Patent.

Respectfully Submitted,

29 July 2008 /Michael A. Glenn/

Michael A. Glenn

Reg. No. 30,176

Customer No. 22862